NIST Advanced Manufacturing Series 300-9

Industrial Wireless Deployments in the Navy Shipyard

Richard Candell
Yongkang Liu
Mohamed Hany
Karl Montgomery

This publication is available free of charge from:
https://doi.org/10.6028/NIST.AMS.300-9

National Institute of Standards and Technology
U.S. Department of Commerce

NIST Advanced Manufacturing Series 300-9

Industrial Wireless Deployments in the Navy Shipyard

Richard Candell
Karl Montgomery
Yongkang Liu
Mohamed Hany

Intelligent Systems Division
Engineering Laboratory

This publication is available free of charge from:
https://doi.org/10.6028/NIST.AMS.300-9

August 2020

U.S. Department of Commerce
Wilbur L. Ross, Jr., Secretary

National Institute of Standards and Technology
Walter Copan, NIST Director and Undersecretary of Commerce for Standards and Technology

National Institute of Standards and Technology Advanced Manufacturing Series 300-9
Natl. Inst. Stand. Technol. Adv. Man. Ser. 300-9, 23 pages (August 2020)

This publication is available free of charge from:
https://doi.org/10.6028/NIST.AMS.300-9

Abstract

The National Institute of Standards and Technology (NIST) and the Office of Naval Research (ONR) have partnered to investigate the application of digital manufacturing methods and technologies within the navy shipyard. As a part of the effort, wireless network deployments are considered. This report provides an overview of the wireless networking requirements of navy shipyards specifically for the transmission of machine information outside and inside of the vessel during construction. Recommended approaches are included with each use case. This report is intended to provide the reader with direction to other larger resources and documentation provided by NIST.

Key words

Industrial Wireless Networks; Smart Manufacturing; Industry 4.0; Industrial Internet of Things (IIoT); Wireless communication; Wireless in Industry; Factory Communications

Table of Contents

1 Introduction 1
1.1 Background 1
1.2 Intended Audience 1
1.3 Scope 1
1.4 Document Organization 1
2 Normative References 2
3 Challenges of Radio Communications 3
3.1 Range 3
3.2 Channel Bandwidth 3
3.3 Information Data Rate (Bandwidth) 3
3.4 Communications Reliability 4
3.5 Latency 4
3.6 Scale 4
3.7 Security 5
3.8 System Availability 5
3.9 Harsh Industrial Environments 6
4 Shipyard Requirements and Recommendations 6
4.1 Shipyard Wireless (Outside the Hull) 6
4.1.1 General Wireless Support 6
4.1.2 Smart Shipyard Site Monitoring 7
4.1.3 Critical Resources Tracking in the Shipyard 8
4.2 Shipyard Wireless (Inside the Hull) 10
4.2.1 Portable Computing Devices Within the Hull 10
4.2.2 Smart Shipyard Sensing and Site Monitoring 11
4.2.3 Drone Use for Ship Hull and Tank Inspection 12
4.2.4 Confined Spaces: Toxic Gas Monitoring 13
5 References 14

List of Tables

Table 1. List of Definitions for Recommendations 6
Table 2. Solution Profile: General Wireless Support 7
Table 3. Solution Profile: Smart Shipyard Site Monitoring 8
Table 4. Solution Profile: Critical Resources Tracking in the Shipyard 9
Table 5. Solution Profile: Portable Computing Devices Within the Hull 11
Table 6. Solution Profile: Smart Shipyard Sensing and Site Monitoring 12
Table 7. Solution Profile: Drone Use for Ship Hull and Tank Inspection 12
Table 8. Solution Profile: Confined Spaces: Toxic Gas Monitoring 13

List of Figures

Figure 1. Active RFID localization for tracking shipyard resources 9
Figure 2. In-hull workspace profiles and wireless networking solutions 10

1 Introduction

1.1 Background

Industry 4.0 and Smart Manufacturing provide a vision of a completely digitally integrated factory in which all machines are connected to an information framework that provides adaptability and visibility not seen before in past industrial evolutions. With the advent of smart manufacturing, the navy shipyard can become more agile to respond to information coming from the command chain and from the shipyard itself. As a part of the digital revolution anticipated for all sectors of manufacturing including that of the shipyard, wireless plays an important role. Radio (i.e. wireless) is a key enabling technology of the vision of the digital factory. Wireless technology enables mobility of personal devices, factory equipment, and machinery such as robots and drones. Wireless also affords a level of capital cost reduction in the massive deployment of sensors and actuators within the factory as it eliminates the need for installation of cables and conduit and the associated labor. Additionally, wireless, coupled with computing resources, enables a degree of autonomy of machinery thereby liberating human resources to perform more interesting and important tasks.

The navy shipyard has user requirements similar to most large manufacturing environments as well as having some more specialized requirements related to security. Thus, the guidance provided to private manufacturing interests also applies to the shipyard. Wireless user requirements of the shipyard include supporting human carried computing devices such as tablets and laptops, machine health monitoring, design upload to cutting machines, inspection of tanks and pipelines using drones, and safety assurance for workers operating in confined spaces. These are only a few of the various user requirements found in the shipyard. These and other use cases are explored within this report.

1.2 Intended Audience

This document is written for the high-level reader interest in seeking guidance on deploying wireless networks in the naval shipyard. The primary audience is for shipyard personnel or people interested in the naval shipyard; however, those interested in requirements and the resulting recommendations will also find benefit in this report The reader should have a basic understand of wireless technologies and how they function and how they benefit the enterprise. Expert understanding of the physics behind radio wave propagation is not required to benefit from the information within this report.

1.3 Scope

This report focuses on providing guidance to shipyard personnel. The document provides a synopsis of the various requirements of the navy shipyard and the guidance provided by NIST to deploy wireless networks in a factory environment. This document only focuses on providing guidance during the construction of the navy vessel. Wireless networks deployed during service of the veseel is not considered within this report.

1.4 Document Organization

This report is organized as follows:

- Section 2 provides normative reference that will be useful for the reader to review;

- Section 3 provides an overview of the challenges in wireless communications in a factory environment;
- Section 4 provides a synopsis of the unique navy shipyard requirements and recommended solutions for each; and, finally,
- Section 5 provides a list of the citations supporting the statements and guidance within the report.

2 Normative References

The following references will be helpful to the reader in understanding the behavior of radio communications and how to deploy industrial wireless network effectively and securely"

1. NIST Guidance on Wireless Deployments. This report provides an overview of radio communications in general with a focus on industrial wireless deployments. A process is recommended which organizations may adopt to better deploy wireless in their specific environments.

   [1] NIST AMS 300-4, *Guide to Industrial Wireless Systems Deployments*, 2018

2. NIST Guidance on Cybersecurity. This report provides the reader with an overview of industrial control systems and recommendations for securing those types of systems.

   [2] NIST 800-82, *Guide to Industrial Control Systems Cybersecurity*, 2015

3. Other NIST publications exist specifically directed toward securing wireless networks. We encourage the reader to utilize the resources of the NIST Computer Security Resource Center online at csrc.nist.gov. The following publication may be of use for the reader; as it provides specific guidance on securing wireless local area networks.

   [3] NIST SP 800-153, *Guidelines for Securing Wireless Local Area Networks*, 2012

3 Challenges of Radio Communications

Radio or wireless communication is defined as the transmission of information such as voice or digital data through the generation of electromagnetic waves modulated according to the information being transmitted. Radio communication, like any other communication technology, is limited by the laws of physics. These laws set the boundaries of how much information can be transmitted, through what, and how far. Some key challenges of a wireless communication system are discussed in the following sections; however the reader is strongly encouraged to download and read NIST AMS-300-4 *Guide to Industrial Wireless Systems Deployments* within which a radio communication primer is provided [1]. Wireless communications is a highly technical field based on electromagnetic theory, information theory, and networking theory. NIST AMS 300-4 was designed to be easily accessible to the lay reader.

3.1 Range

The distance over which radio waves can travel is constrained by the distance, obstacles, and fundamental wavelengths (or frequency) used by the communication system. The greater the distance, the weaker the transmitted signal becomes and the higher likelihood for information loss due to noise in the receiving electronics and outside influences. Obstacles such as metal and concrete severely attenuate radio waves thus making information loss more likely as well. Radio waves lose power (attenuate) faster as the frequency of the transmission increases, therefore, higher frequency systems will generally have better throughput performance but with less range than systems operating in the lower frequency bands. As an example, a wireless system operating a 2.4 GHz will generally have greater range than a system operating at 30 GHz, but the bandwidths of the 2.4 GHz system will be less. The antenna design, the electronics, and signal process capability of the receiver will determine how weak a wireless signal can be before information loss occurs.

3.2 Channel Bandwidth

Wireless communications systems transmit their information over finite resources within the electromagnetic (EM) spectrum. The EM spectrum is a limited natural resource which has been logically divided according to the laws and regulations of each world nation. Each communications system utilizes a portion of the EM spectrum for transmission of information. That portion of the spectrum utilized occupies a finite amount of space within the spectrum called “channel bandwidth” which is a main limiting factor through which information can flow. The limit of information flow through the channel is mathematically governed by Shannon’s channel capacity equation [4] which states that the amount of information flowing through a wireless channel is theoretically limited by bandwidth and noise and is impossible to surpass.

3.3 Information Data Rate (Bandwidth)

The amount of information that can be transmitted at any one time defines a communication system’s bandwidth or data rate. Bandwidth is defined in terms of bits per second and is constrained by the physics of the communications channel, i.e. channel bandwidth, signal-to-noise-plus-interference ratio (SNIR), etc. Communications equipment manufacturers understand these constraints, and design and market their products accordingly. Therefore, each system of devices will be marketed by a maximum bandwidth possible under pristine channel conditions. Realizable bandwidth rarely meets

the advertised data rates as channel conditions introduce error, and competition for the channel by other devices on the wireless network creates delay in channel access.

3.4 Communications Reliability

The communications reliability performance of a wireless system is largely determined by the signal-to-noise (SNR) ratio and the signal-to-interference ratio (SIR) of the information-bearing radio waves at the receiver. Noise and interference sources contribute to the overall degradation of the transmitted radio waves and ultimately lead to a loss of information as the noise and/or interference overcome the intended signal. Interference can also be considered a form of noise and hence both noise and interference are often considered together through SNIR. All wireless systems have a minimum SNIR for which information transfer is no longer possible. Additionally, all systems have a minimum threshold of SNIR for error-free communications. Theoretically, it is impossible for any communication system to operate error-free for any amount of time; however, modern communication has advanced such that some wireless systems are able to perform well in the presence of significant amounts of noise. Most communications systems such as Wi-Fi (IEEE 802.11) and cellular communications systems reduce information performance to continue to operate as SNIR decreases. Steps may be taken to improve SNIR performance. For example, wireless stations should not be placed too far away from the stations with which they communicate. In a Wi-Fi network, locating stations within 50 m is recommended. Second, interference sources can be managed through policy and spectrum awareness. Understanding and limiting sources of interference is necessary. Microwave ovens can cause considerable harm to a wireless network operating at 2.4 GHz. Finally, deploying a spectrum monitoring system to detect sources of interference and jamming is recommended for any mission critical system. Commercial spectrum monitoring systems are available within the marketplace. It is also relatively easy to build a spectrum monitoring system using open source components [5].

3.5 Latency

In any communication system, time is required to transmit and receive data. In a wireless system, the data for transmission must be provided by the software application, formatted for transmission, modulated, and transmitted. Then, the electromagnetic waves take time to propagate through space at the speed of light which is approximately 0.3 meters per nanosecond. Propagation time is usually negligible within the domain of a factory[1]. Once the radio waves arrive at the receiver, additional time is required to detect the signal, reconstruct the signal into information usable by the application, and then finally delivered to the user software application. Latency is defined as the actualized duration of information transmission from one application to another within an industrial control system [6]. Often latency is measured as the round-trip duration from interrogation to response as with *ping* utility.

3.6 Scale

A wireless network is designed to support a certain number of devices. The number of devices supportable within a wireless network is called scale. Scale is an important factor of an industrial wireless networks as it influences the amount of time expected for devices to utilize the finite

[1] Propogation time is only important to those systems with latency constraints under 1 μs. Most industrial systems do not require sub-microsecond latency but rather require latencies between 1 and 100 ms.

resources of the wireless channel. As the number of devices on a network increases, channel contention in some types of network implementations will occur. Determinism of latency may be affected. Some wireless systems such as WirelessHART and ISA100.11a employ scheduling to assure channel availability. Other wireless systems such as Wi-Fi use a random-access scheme to access the channel, and, in those types of systems, channel access is not assured within a deterministic amount of time. Work is underway currently within the IEEE 802.11 standard committee to study the implementation of time-sensitive networking (TSN) to apply various forms of transmission scheduling within the Wi-Fi network. Other proprietary IEEE 802.11 implementations have been produced and are not considered Wi-Fi compliant.

3.7 Security

This document is not to be used as a normative reference for security. The reader is strongly encouraged to consult the NIST suite of cyber-security recommendations and guidance listed in the normative references section of the introduction.

Security within any industrial wireless deployment, especially those considered mission critical, should always be considered jointly with the design of the wireless network and mission application. Security holistically addresses the concerns of data confidentiality, integrity, and availability. Security does not only consider encryption for data confidentiality. Unlike a typical office environment, in an industrial wireless network, data integrity and availability are of equal or at times are of greater concern than confidentiality. It should be noted that data confidentiality is of utmost concern when proprietary or classified design information is transmitted to fabricating machinery within the shipyard. Strong encryption is available for most modern wireless networks and should be used within the shipyard. To ensure authentication of devices on the wireless, authentication protocols should be used to verify access.

Wireless networks are also vulnerable to transmission attacks, meaning jamming attacks. In mission critical systems, isolating the wireless network through frequency and distance is recommended. Additionally, a distributed spectrum monitoring system within localization functionality supported by small drones for inspection of spectrum intrusion is recommended.

3.8 System Availability

The ability of a wireless network to support its intended operation for an amount of time without failure is referred to as system availability. This is typically defined in terms of a percentage availability, such as 99.99%, for which it will stay operational and support its intended mission. Increasing the numbers of nines decreases service interruption but usually increases cost and complexity of the system as levels of redundancy in both hardware and software are necessary. System availability refers to the components of the wireless network such as routers, switches, and stations and should not be confused with communication reliability. System availability of a wireless network is more often impacted by the hardware used to support the network rather than events occurring within the electromagnetic environments. Therefore, attention should be placed on the robustness of the devices within the network and the speed at which a network can recover from power outages, software glitches, etc. Many networks, such as wireless sensor networks recover very slowly after loss of power of an access point. Some products cache network information to allow for a speedy recovery, and others do not. Therefore, care should be placed during the candidate selection process. This is explained within NIST AMS 300-4 [1].

3.9 Harsh Industrial Environments

Typically, the physical environment impacts wireless communications transmissions through obstructions, reflections, and scattering. These impacts lead to having multipath transmissions that sometimes may not have a direct line-of-sight (LOS) component. Compared to office and home environments, industrial environments are more electrically noisy and present many more obstructions and disruptions to wireless transmissions. Examples of this harsh environment include moving metal objects such as forklifts and cranes, narrow aisles between metal shelves, and liquid tanks that can alternate the propagation characteristics. Moreover, electrical noise can have an impact on wireless transmissions depending on the frequency of the generated noise. Examples of low frequency noise sources include motors and solenoids. Higher frequency electrical noise can be generated by arc generating equipment.

4 Shipyard Requirements and Recommendations

This section provides a synopsis of the various industrial wireless user requirements found in the navy shipyard. Within each subsection, a description of the shipyard use case is described. Each use case is accompanied with a set of recommendations.

Table 1. List of Definitions for Recommendations

Network Type	Description	Examples
WLAN	Wireless Local Area Network	Wi-Fi (infrastructure mode)
ADHOC	Ad-hoc wireless local area network	Wi-Fi ad-hoc mode, stationary (not MANET)
WSN	Wireless sensor network	Industrial Mesh: ISA100.11a, WirelessHART, Zigbee, Proprietary
PAN	Personal area networks	Bluetooth, Wireless USB
RFID	Radio frequency identification	ISO 18000
LPWAN	Low-power wide area network	Narrowband IoT, Sigfox, LoRaWAN
CELL	Cellular networks	3GPP-based systems such as LTE and 5G

4.1 Shipyard Wireless (Outside the Hull)

4.1.1 General Wireless Support

General wireless support for personal portable devices such as laptops, tablets, and cellphones is well-studied. Most wireless local area networks (LANs) employ Wi-Fi using lightweight access points (distributed antennas) throughout a domain. Within factories, wireless LAN has been used successfully and securely using this approach; therefore, this report recommends such an approach for the shipyard outside of the hull.

Table 2. Solution Profile: General Wireless Support

Network Type	WLAN (Wi-Fi)
Topology	Infrastructure Mode, High gain sectorized antennas[2]
Use Cases	Personal portable devices such as laptops, tablets, and smart phones; cutting machines outside the hull for machine prognostics and health monitoring
Frequency Band	2.4 GHz (for range), 5 GHz or 6 GHz for range or for better isolation from noise source emanating from machinery, personal devices, etc.

4.1.2 Smart Shipyard Site Monitoring

Smart monitoring has been widely deployed in many fields including home, office, and industrial environments. Shipyard site monitoring use cases include alarming systems, video surveillance, sensing systems, and machine health monitoring. Additionally, the data collected by various tracking applications, and schedule and progress monitoring are also considered part of the site monitoring. In this section, we focus on sensing applications in site monitoring while the other site monitoring applications are considered part of general wireless support as discussed in Section 4.1.1. Outside the hull, site monitoring sensing applications include general properties such as the temperature, pressure, and humidity, and task-related quantities such as air quality, gas levels, piping inspection, surface painting and coating process, and fluid level in tanks [7]. Moreover, the metal processing can be monitored through introducing massive sensing capabilities for automated casting, forging, rolling, cutting, welding or cleaning.

Wireless sensor network (WSN) protocols are used for task-related applications deploying IEEE802.15.4 based protocols such as WirelessHART, ISA100.11a, and ZigBee. The selection of these protocols is mainly because of the existence of industrial grade and low-cost nodes that can satisfy the low power and the low data rate requirements of shipyard sensing applications. Typically, the WSN can fulfill the data rate requirements of condition monitoring, open loop control, and regulatory closed loop control by having a data rate that is at least four times faster than the time constant of the underlying processes. The typical range of coverage is around 60 meters and mulithop communication can extend the range through relay devices. The required reliability of these networks is achieved through allowing redundant information paths through different nodes (using a mesh topology), the network gateway ability of identifying path quality, and the use of Frequency Hopping Spread Spectrum (FHSS) and Direct Sequence Spread Spectrum (DSSS). Finally, the battery life for nodes in these networks generally can be five years or more depending on the update rate. As a result, battery-powered and low rate sensors can be used in different communications modes to monitor the shipyard site.

[2] This assumes wall-mounted antennas. Sectorized antennas are patch arrays, horns, or similar antenna configuration. Omni-directional or toroidal beam pattern antennas are not recommended unless warranted by installation location of the antenna such as a hanging location in the center of the coverage area.

Table 3. Solution Profile: Smart Shipyard Site Monitoring

Network Type	WSN
Topology	Star, mesh, hybrid star/mesh within routing nodes liberally dispersed throughout the yard to assure performance
Use Cases	Sensing for air quality, gas levels, piping inspection, and fluid level in tanks
Frequency Band	900 MHz (preferred) or 2.4 GHz

4.1.3 Critical Resources Tracking in the Shipyard

The shipyard needs to track critical on-site resources, e.g., high-value tools, transportation vehicles, and vessel equipment, whose location information is used in the inventory check and schedule planning as shown in Figure 1. The tracked object can move in both indoor and outdoor areas, which means the wireless tracking service should cover all possible places in the shipyard. For an outdoor object, global positioning system (GPS) signals are sufficient to accurately obtain its real-time position. However, such information is only available when the tracked object has a GPS receiver and clear visibility to the sky. It also needs to routinely report its location to the centralized management system via wireless data links, such as the general wireless support as discussed in Section 4.1.1. The GPS reception may degrade or become completely lost in the indoor cases. Therefore, an indoor wireless localization system is also needed. Wireless localization solutions, e.g., using Wi-Fi or Bluetooth networks, provide options with the required accuracy for tracking objects. However, as the radio module of the tracked object is normally powered by batteries, Wi-Fi or Bluetooth devices can only work for hours between two consecutive charges, which cannot support a long standby time that is typically required on a tracking service, e.g., for months. Carrier-grade cellular networks can also provide localization services for conventional cellular devices and IoT devices, e.g., NB-IoT terminals. However, cellular localization solutions rely on the options from local service providers whose availability and capacity of the cellular infrastructure may vary with shipyard locations.

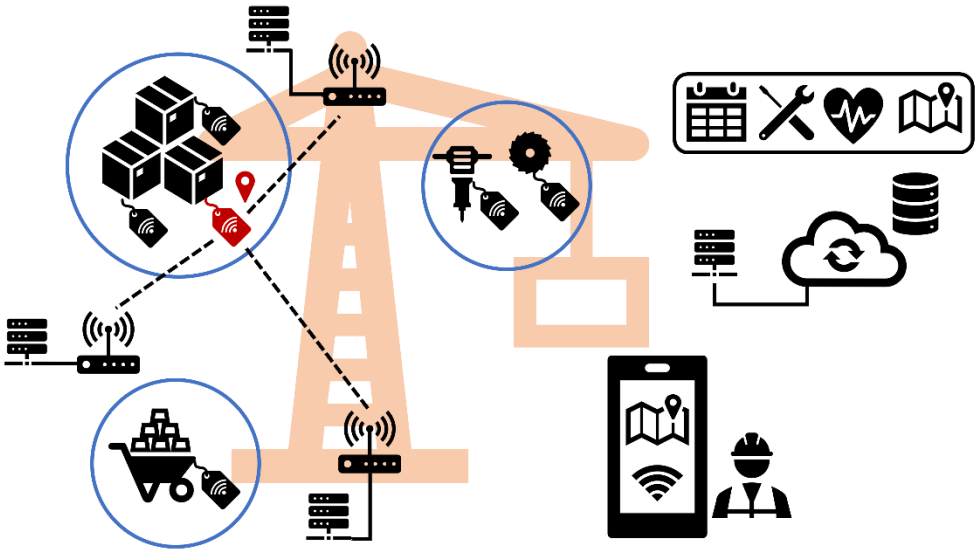


Figure 1. Active RFID localization for tracking shipyard resources

Radio-frequency identification (RFID) provides a low-cost and low-energy tracking solution that can be self-installed and managed as part of the shipyard information technology (IT) architecture. One RFID tag can send a small amount of data that contains a sequence number or a uniform resource identifier (URI) to the transponder. Such short information is linked with one record entity in the database that points to the object that is physically attached. Active RFID tags, powered by on-board batteries, often have an effective read range of more than 100 m [8]. A typical RFID localization system can deploy multiple transponders as a multi-dimensional grid in the service area whose positions are fixed and known to the central controller. The transponder density should be high enough, i.e., any tag in the area can communicate with three or more transponders so that the signal data can localize the tag's geometrical position. The central controller schedules transponders in scanning the tags and updates their locations in the database routinely or upon request. The field operator can be guided to the tracked object by the instant navigation information from an portable computing device that receives the location update from the server. The tag can be further verified using a portable RFID reader when it is approached.

Table 4. Solution Profile: Critical Resources Tracking in the Shipyard

Network Type	RFID
Topology	Infrastructure mode interrogation, using active tags
Use Cases	Object tracking, inventory check
Frequency Band	Depends on the manufacturer, e.g., 2450–5800 MHz ISM for active tags[3]

[3] Interference from a WLAN is not considered. Careful frequency planning is necessary to ensure performance of RFID tag interrogation

4.2 Shipyard Wireless (Inside the Hull)

4.2.1 Portable Computing Devices Within the Hull

Within the ship hull, field operators rely on their portable computing devices, e.g., smartphones, tablets, and laptops, to keep their workspace connected to the shipyard data pool or external resources, in use cases such as data entry and retrieval with on-premises or cloud servers, augmented reality with remote diagnosis and instruction, or voice/video/message services for task coordination. The metal ship hull usually blocks these devices from directly using the shipyard wireless network. Therefore, new wireless networking solutions are needed to serve them within the hull.

A ship construction/maintenance project may last for days, months, or even years. Field operations may also be performed under different situations within the hull. As shown in Figure 2, three in-hull workspace profiles are identified regarding available networking and utility supports. Solutions for different profiles are proposed, respectively, to enable wireless communications between portable computing devices and outside nodes.

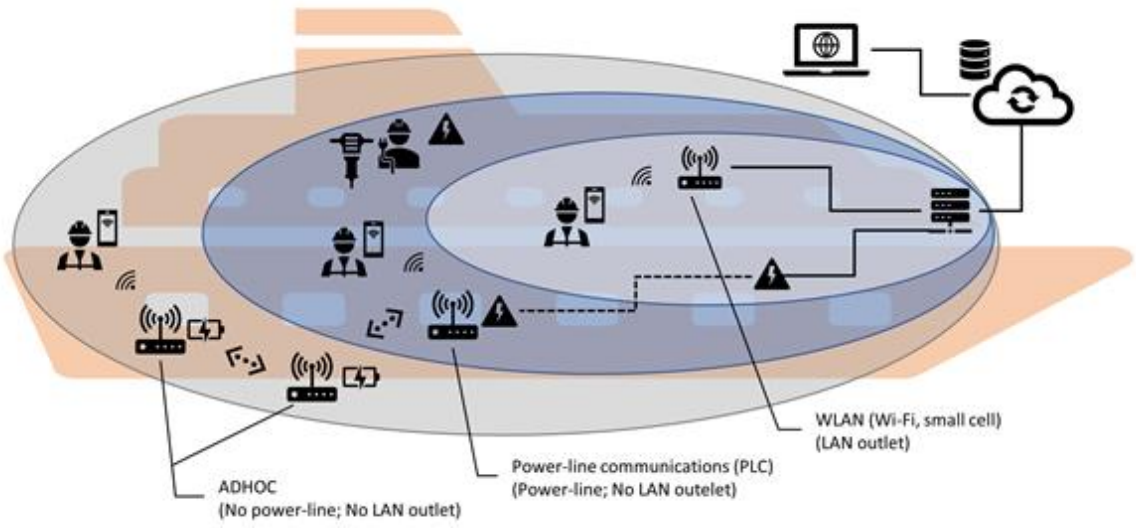


Figure 2. In-hull workspace profiles and wireless networking solutions

If the workspace has available wired network connections, e.g., an Ethernet-based network that can reach the shipyard network infrastructure, a WLAN access point may be installed by by replacing the Ethernet cable with a WLAN connection. The access point may be powered by the same power-line supply used for general power.

If the workspace only has a power line that is connected to the shipyard power grid, without any data outlet, a power-line communication link can be created between two AC power outlets, one in the workspace and another near the external data outlet. Power-line communication modems are used at both outlets that transmit data signals following the IEEE 1901 standard to use the existing circuit as the wired data cable. The external modem is plugged into the network infrastructure; the internal one is connected to a WLAN access point that creates a Wi-Fi hotspot.

If the workspace is either unfinished or confined with no data outlet or power line to the external facility, a multi-hop wireless relay path can be deployed to extend network connections from one of

the nearest data outlets, e.g., a WLAN hotspot or a wired network terminal. Intermediate relay nodes which are battery powered can work together to form a wireless ADHOC backbone, each of which then serves as a hotspot in its own covered workspace for wireless devices. Data transmitted in the backbone and hotspots can be assigned in different frequency bands, e.g., 2.4 GHz for the backbone and 5 GHz for the hotspots. The link quality between relay nodes can be further enhanced by using the multiple-input multiple-output (MIMO) technique[4].

Table 5. Solution Profile: Portable Computing Devices Within the Hull

Network Type	Wi-Fi hotspot
Topology	Star in a Wi-Fi hotspot. Wi-Fi access points reach the shipyard network infrastructure through data outlets, point-to-point power-line communication links, or an ADHOC wireless backbone. Low-cost edge computers with built-in WLAN support and MIMO antennas can be placed through the ship to be used as the ADHOC backbone.
End Device	Laptop, tablet, smart phone
Frequency Band	2.4 GHz and 5 GHz ISM

4.2.2 Smart Shipyard Sensing and Site Monitoring

Similar to the site monitoring scenarios outside the ship hull as described in Section 4.1.2, the monitoring inside the hull for sensing applications will follow. The major difference of the proposed solution is that a multihop IEEE802.15.4 based wireless sensor network (WSN) would be deployed. The placement of relay nodes should be designed according to the ship's layout with routing nodes liberally placed throughout especially at spatial junctions within the hull such as portals. Battery powered sensor nodes exist that allow for ease of installation and portability; however, if wired power is available, it is recommended to use that power especially for nodes with a large amount routing traffic.

[4] IEEE 802.11ac supports up to 8 spatial streams; however, this does not assure product availability in the market. It should be possible to implement 4x4 minimum in ad-hoc mode with a PCI-based Wi-Fi card and an external 4-port antenna system. The end device would not have 4 antenna ports, but the ad-hoc infrastructure would.

Table 6. Solution Profile: Smart Shipyard Sensing and Site Monitoring

Network Type	WSN
Topology	Star, mesh, hybrid star/mesh within routing nodes liberally dispersed throughout the hull to assure performance
Frequency Band	2.4 GHz

4.2.3 Drone Use for Ship Hull and Tank Inspection

Drone use for inspections is a nondestructive evaluation (NDE) method to detect corrosion, cracks, and other issues that may undermine safety, performance, and cost. Utilizing remote controlled drones for inspection reduces time spent during the preparation for and the performance of inspections. Drones reduce the level of danger to the inspector – the risk is shifted from the inspector, who would otherwise be required to scale the walls of a ship hull or a large tank, to the drone itself. In terms of communications, drones aid in the inspection process by transmitting pictures, videos, and other sensor data to the inspector, eliminating the need to construct and traverse scaffolding. A reference describing drone use for a wide range of industrial inspections and applications may found in [9]. Requirements for the wireless technology solution for this use case include: 1) maintaining line of sight (LOS) as much as possible; 2) assuring a usable range between the drone and operator; and 3) assuring the support of video, control, and other sensor data streams. These requirements are developed to assure reliable communications for the control, video, and sensor data streams.

Table 7. Solution Profile: Drone Use for Ship Hull and Tank Inspection

Network Type	WLAN (Wi-Fi)
Topology	Infrastructure mode[5]
Use Cases	Visual, sonar, and ultrasound inspection of large tanks inside and outside the tank; inspection of the hull inside and outside the ship.
Frequency Band	2.4 GHz (control stream), 5 GHz (video and sensor streams)

The solution profile in Table 7 utilizes WLAN (Wi-Fi) in the 2.4 GHz ISM band for the control stream and the 5 GHz ISM band for the video and sensor streams[6]. An advantage with WLAN compared to other wireless communication protocols is the wide range of compatibility with other Wi-Fi enabled devices and sensors.

[5] When WLAN is used for drone control or media transmission, the drone usually serves as the access point with the controller serving as the client/station.

[6] With the advent of 6 GHz ISM, it may be possible to use 6 GHz; however, it should be noted that range usually suffers as the transmission frequency is increased.

Examples of Wi-Fi enabled devices and sensors include sonar sensors, ultrasound sensors, and thermal cameras. A common practice is to configure the drone to transmit and receive the control stream on one frequency band and use another frequency band for video and sensor streams. Using separate frequency bands for the control stream and the video/sensor streams prevents co-channel interference from the same device. This lack of interference in the control stream increases overall reliability. To ensure LOS between the drone and the inspector in a harsh radio environment, remove or avoid objects that may reside in the first Fresnel zone depicted in the Quick Start Guide, Appendix A. Ensuring LOS using WLAN provides ample range for the most common distances between an inspector and the drone; however, the highly reflective environment of the shipyard could be leveraged to extend range in non-LOS situations. Drones are typically configured using the infrastructure mode topology in which the drone acts as a flying access point. The remote control device and the remote video display are wirelessly linked to the drone utilizing the 2.4 GHz and 5 GHz bands, respectively. In selecting the optimal wireless solution, frequency planning [1] should be conducted in the shipyard so that if the 2.4 GHz band is too heavily utilized, consider moving the frequency of the control stream to a predefined channel in the 5 GHz band that has the lowest interference.

4.2.4 Confined Spaces: Toxic Gas Monitoring

Generally, one of the main causes of accidents in confined industrial spaces is the accumulation of dangerous gases. Various hazards are considered in confined space monitoring such as oxygen depletion, and toxic and combustible gases accumulations. In shipbuilding, toxic gases from welding, soldering and thermal cutting processes are a main source of accidents and are associated with many adverse health effects. In shipbuilding, the working space is not fixed and metal structures throughout the ship exist such that portable gas detectors are necessary. A wireless multihop toxic gas remote monitoring system may be used to communicate with a safety control station with response time satisfying the maximum exposure times assuring safety protocols for toxic gases.

Table 8. Solution Profile: Confined Spaces: Toxic Gas Monitoring

Network Type	WSN
Topology	WSN mesh/star; Some wearable sensing products are available using Bluetooth; NIST has performed a reliability study of gas sensing using ISA100.11a [10].
Frequency Band	900 MHz (preferred) or 2.4 GHz

The proposed solution includes a multihop IEEE802.15.4 based WSN. The reasons behind selecting these networks are briefly discussed in section 4.1.2. The placement of relay nodes should be designed according to the ship's layout. The operating frequency should be selected to coexist with other wireless systems in the ship according to the frequency plan of the shipyard. The WSN protocol allows for dynamic mesh routing to recover from node failures and change the routes dynamically with the movement of the portable sensor node. Battery powered sensor nodes exist that allow for ease of installation and portability. Examples of protocols that satisfies gas detection requirements include WirelessHART, ISA100.11a, and ZigBee [10] [11].

5 References

The following references were used in developing this report.

[1] R. Candell, M. Hany, K. B. Lee, Y. Liu, J. Quimby, and K. Remley, "Guide to industrial wireless systems deployments," Gaithersburg, MD, Apr. 2018. doi: 10.6028/NIST.AMS.300-4.

[2] K. Stouffer, V. Pillitteri, S. Lightman, M. Abrams, and A. Hahn, "Guide to Industrial Control Systems (ICS) Security," Gaithersburg, MD, Jun. 2015. doi: 10.6028/NIST.SP.800-82r2.

[3] M. Souppaya and K. Scarfone, "Guidelines for securing wireless local area networks (WLANS)," in *Bluetooth and Wireless Local Area Networks: Security Guides*, 2013.

[4] C. E. Shannon, "A Mathematical Theory of Communication," *Bell Syst. Tech. J.*, 1948, doi: 10.1002/j.1538-7305.1948.tb01338.x.

[5] R. Candell, "Requirements for Spectrum Monitoring in Industrial Environments," *NIST Interagency/Internal Report (NISTIR)*. .

[6] K. Montgomery, R. Candell, Y. Liu, and M. Hany, "Wireless User Requirements for the Factory Work-cell," 2019. doi: https://doi.org/10.6028/NIST.AMS.300-8.

[7] P. Fraga-Lamas, D. Noceda-Davila, T. Fernández-Caramés, M. Díaz-Bouza, and M. Vilar-Montesinos, "Smart Pipe System for a Shipyard 4.0," *Sensors*, vol. 16, no. 12, p. 2186, Dec. 2016, doi: 10.3390/s16122186.

[8] J. Zhou and J. Shi, "RFID localization algorithms and applications—a review," *J. Intell. Manuf.*, vol. 20, no. 6, p. 695, 2008, doi: 10.1007/s10845-008-0158-5.

[9] "Drone Inspections A Comprehensive Guide to How Drones Are Being Used for Visual Inspections throughout the World," 2020. https://www.flyability.com/drone-inspections (accessed Apr. 22, 2020).

[10] M. T. Hany and R. Candell, "Industrial Wireless End-to-End Measurements and Impacts in a Gas Sensing Scenario," *J. Res. (NIST JRES)-*, vol. 123, no. J. Res. (NIST JRES)-, 2018.

[11] C. Pérez-Garrido, F. González-Castaño, D. Chaves-Díeguez, and P. Rodríguez-Hernández, "Wireless Remote Monitoring of Toxic Gases in Shipbuilding," *Sensors*, vol. 14, no. 2, pp. 2981–3000, Feb. 2014, doi: 10.3390/s140202981.

Appendix A:
Quick Start Guide

The “Industrial Wireless Deployment Lifecycle Quick Start Guide” is a two-page infographic that aids in the understanding of the wireless lifecycle process presented in NIST Advanced Manufacturing Series 300-4, “Guide to Industrial Wireless Systems Deployments” [1]. The first page of the Quick Start Guide provides a general overview. The second page provides a simplified solution utilizing the industrial wireless deployment lifecycle for the specific use case: “Enabling Wireless Support for Portable Devices Within the Ship Hull During the Construction Process.” This guide provides references that point the reader to specific chapters and sections from NIST AMS 300-4. Please note that references used in the Quick Start Guide point to chapters and sections in NIST AMS 300-4.

Industrial Wireless Deployment Lifecycle Quick Start Guide

Industrial Wireless Fundamentals

2.1 Industrial Control Systems

Continuous Processes
- Flow based
- Batch Based

Discrete Manufacturing
- Job-based

2.2 Current Wireless Techonolgy

Home and Office
- IEEE 802.11 (Wi-Fi)

Instrumentation
- IEEE 802.15.4
  - ISA 100.11a
  - WirelessHart
  - Zigbee

2.3 Wireless Networking Basics

Radio Frequency (RF) Communications
- Antenna Placement
- EM properties

Networking
- Star Pattern
- Mesh

2.4 Wireless Applicability and Challenges

Requirements: Dependent on each application
- Latency
- Probability of transmission failure
- Scale (# nodes)

2.5 Electromagnetic (EM) Spectrum Guidance

Spectrum Planning
- Licenced
- Unlicensed bands
  - Easy to work with
  - Many interference sources

All References Refer to: NIST AMS 300-4

Chapter 2

2.1 – **Industrial Control Systems** defined as data acquisition, instrumentation and control systems, and the human interface
2.2 –**Wireless technologies**, such as Wi-Fi and ZigBee, with corresponding domains of use
- **Appendix B** is a wireless technology applicability matrix

2.3 – Definitions, concepts, and considerations for **wireless communications and networking**
2.4 – **Wireless Requirements**
2.5 – **Spectrum governance** considerations

Node Placement: Overcoming Shadowing

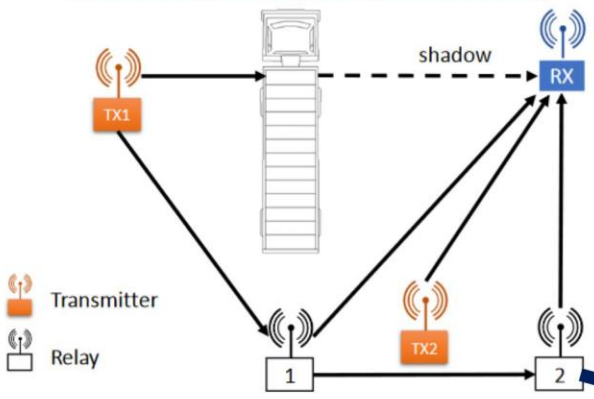


Figure 14. Overcoming Shadowing

First Fresnel Distance Zone (F_1)

$$F_1 = \sqrt{\lambda d_1 d_2 / (d_1 + d_2)}$$

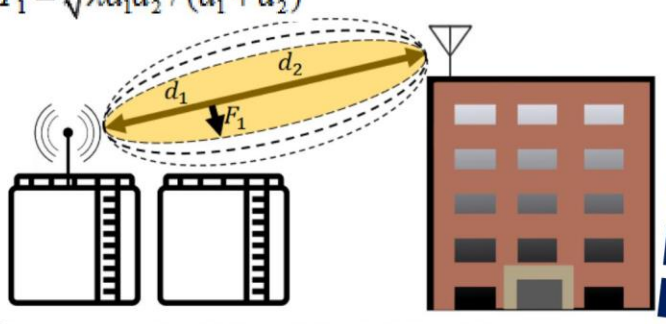


Figure 13. Antenna Height using the Fresnel Distance

Section 7.1

- To increase reliability, ensure **Line of Sight (LOS)** between the transmitter and receiver with **no obstructions in F_1**

Section 7.2

- **Path redundancy** leads to reliability improvement
- Utilize **relays to overcome shadowing** by objects

Spectrum Planning

- **Minimize Interference** by selecting available frequency bands and channels
- **Have knowledge** of devices that can emit interference
  - Microwaves
  - Smart Phones

Spectral Activity in Unlicensed 2.4Ghz Band

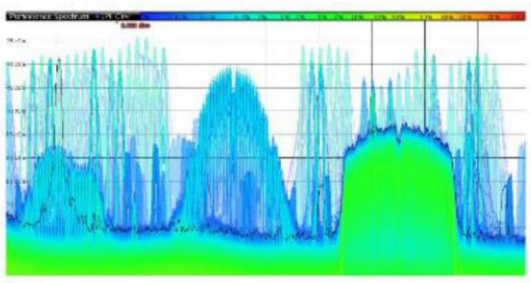


Figure 4. Spectral activity in the 2.4 GHz ISM Band

Section 2.3.1

- RF communication, electromagnetic properties, spectrum activity, and measurement techniques

Section 2.5.2

- Licensed and unlicensed bands. Internal governance by an elected governing board for spectrum management

Industrial Wireless Deployment Lifecycle

4.1 What needs to be acomplished?

Define Objectives
- Define Purpose
- Manage Risk
- Control Expectations
- Involve the Stakeholders

4.2 Where will the wireless system be deployed?

Factory Survey
- Spectrum utilization
- Interference
- Factory Model
- Software

4.3 What wireless techonolgy should be used?

Select Candidates
- Vendor Survey
- Validation
- Band Selection
- Training
- Regulatory

4.4 How is a plan made?

Design a Solution
- RF Survey
- Spectrum Allocation
- Simulation
- Testing

4.5 How can the solution be tested?

Deploy & Monitor
- Iterative deployment
- Spare parts
- Monitoring

Note: Deployment typically occurs after iteration and validation.

Iterative Process

Chapter 4

- Each Stage of Lifecycle highly detailed in **4.1-4.5**
  - Iterative process that relies on previous stage

Appendix A-1 → A-6

- All stages of the lifecycle correspond to a **Checklist A-1 →A-6** to aid in the wireless lifecycle progress

Industrial Wireless Security

- **IT Systems** – Need security for Confidentiality
- **OT Systems** – Need security for Availability

Practical Considerations:
- Physical security
- Spectrum monitoring for malicious actors
- Network Monitoring

Wireless for Safety

- **Wireless safety systems** are used in many applications:
  - Preventing chemical handling mishaps
  - Avoiding heavy equipment accidents
  - Preventing falls through active position monitoring and safety interconnects
  - Situational awareness within confined spaces
  - Improving safety for non-employees

Chapter 5

- **SIL rating** for safety
- Advantages of wireless for safety

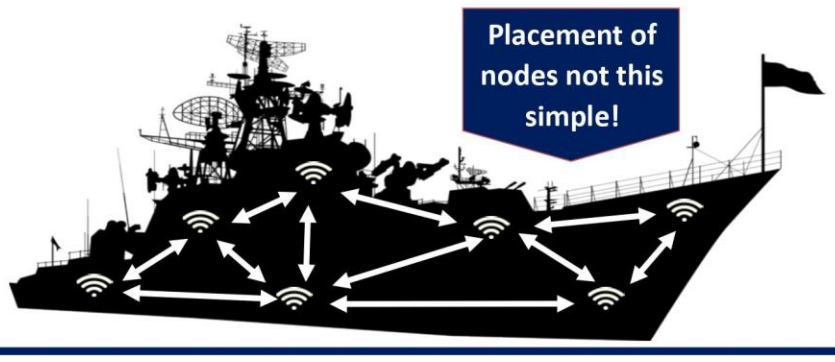
Chapter 6

- Other **practical considerations** for security also discussed
- **Normative Security References:**
  - Section 6.3

NIST
National Institute of Standards and Technology

Utilizing the Industrial Wireless Deployment Lifecycle

Use Case: Enabling Wireless Support for Portable Devices Within the Ship Hull During the Construction Process



Motivation

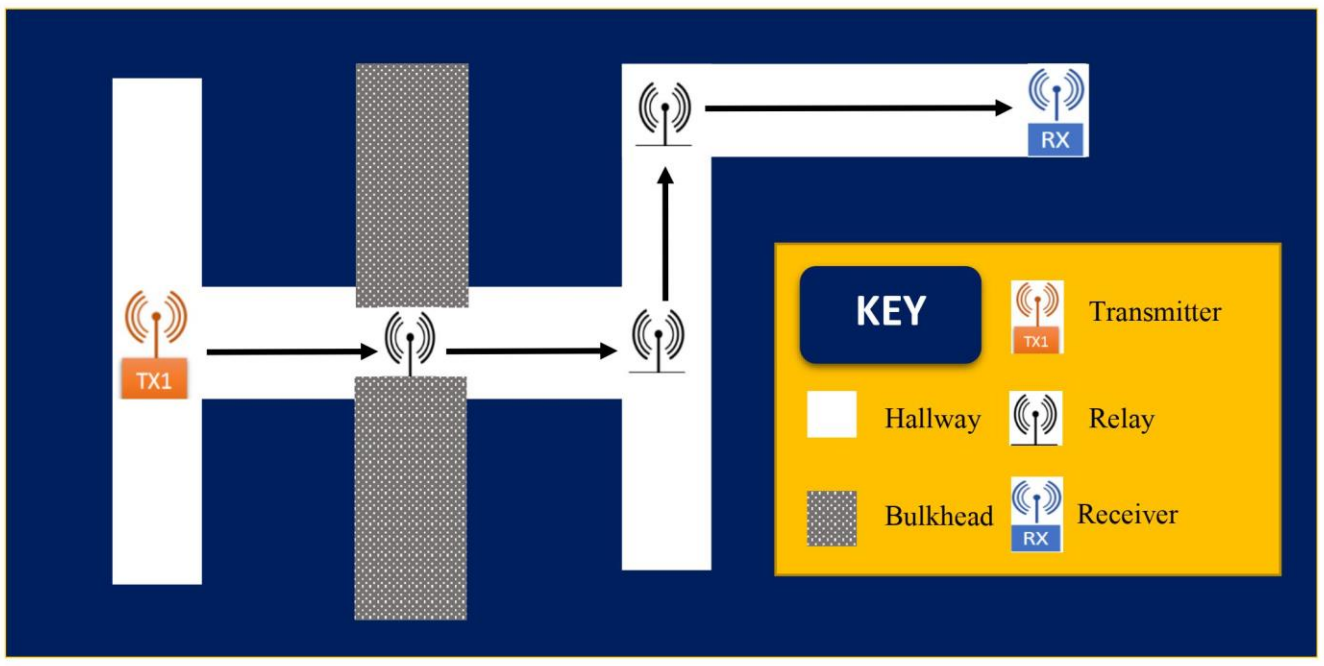
- This Use Case is presented as an example of how a solution can be developed utilizing the industrial wireless lifecycle
- The Use Case represents a real-world problem. A simplified solution to the Use Case is presented below

Industrial Wireless Deployment Lifecycle

4.1 What needs to be acomplished?	4.2 Where will the wireless system be deployed?	4.3 What wireless techonolgy should be used?	4.4 How is a plan made?	4.5 How can the solution be tested?
Define Objectives • **Access to internet** using portable devices within ship hull during the building process • **Dynamically change network** as building proceeds • **Consultation of stakeholders** including network engineers	**Factory Survey** • **Electromagnetic environment** is very confined as the metal walls in the hallways and bulkheads reflect RF signals • **Ensuring LOS** is critical in this use case due to the harsh RF environment	**Select Candidates** • **IEEE 802.11 (Wi-Fi) s**elected due to network **requirements** from the end user devices and accesable hardware • Band and channel selection determined with **Spectrum Planning**	**Design a Solution** • Solution requires **LOS** for all wireless links between transmitters, relays, and receivers • **Simulation** is possible; however, not needed for this simplified solution	**Deploy & Monitor** • The design and approach to the solution may be tested in a **small,** then **large scale test,** to validate performance • **Iteration** used to modify solution • Deployment after validation

Iterative Process

Simplified Solution: Top view map of Hallways and Bulkhead inside ship during building process



Next Steps to Deployment

Select Hardware

- Transmitters, receivers, and relays should be selected to match the simplified solution map
- Selections include: **Wireless routers**, **user devices** (such as tablets), and Wi-Fi **range extenders**

Perform Small-Scale Test

- A small-scale test will be used to validate the simplified solution concept and evaluate user device requirements
- Iteration at this step may be necessary to progress to a large-scale test

Perform Large-Scale Test

- A large-scale test is used to provide analysis regarding network bottlenecks and coverage issues
- Monitoring and analysis is performed to measure the EM spectrum, network traffic, and status of security.

National Institute of Standards and Technology

References and Citations in NIST AMS 300-4

Chapter 4

4.1 – To assess the wireless requirements, objectives should be defined with the consultation of **stakeholders**
4.2 – This solution does not account for **physical inventory in an environment** that may change the placement of nodes
4.3 – Technical and network requirements should be considered
4.4 – Specification of network architecture in this stage. Steps include planning analysis, design, simulation, and optimization
4.5 – Validation of a solution through performance evaluation

Section 4.4.1

- Solution uses 2.4 or 5 GHz ISM bands. **Spectrum Planning** is required for selection
  - 2.4 GHz band has better range; however, many legacy devices use this frequency band leading to higher interference

Section 4.4.3

- Quality of Service **(QOS) performance evaluation** to produce QOS heat map

Section 4.4.5

- **Topology** and **node placement**
  - Brittle topology can create network bottlenecks

Section 4.5.1

- Steps to a successful wireless deployment
  - **Deployment**
  - **Monitoring and Analysis**
  - **Updating and Optimizing**
- Guidance on antenna positioning and characteristics

Section 4.5.2

- Several **types of monitoring** provided in **4.5.2.1-4.5.2.4**
- Dynamic networks
  - Addition and subtraction of nodes in time